Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 4 | Apr 2017

SECURITY USING GEO-ENCRYPTION

Saloni Dhuru [1] | Shraddha R. H. [1] | Meghna Jain [1] | Akshata Lad [1] | Neena Jacob [1]

[1] SIES Graduate School of Technology, Navi Mumbai, India.

ABSTRACT

The location based encryption or Geo-Encryption technique that uses GPS technology to enhance the data security. This concept is developed so that at a particular position and time, the specific recipient will decrypt the files. This technology will be used to restrict unauthorized user for any violation. The approach is to use a security system to secure data by using an encryption algorithm and particular coordinates of the recipient with tolerance distance. It will set a limit to decrypt that encrypted data. It is an innovative technique to encode the location information into the encrypted keys. If an unauthorized person attempts to decrypt the file at some other location, the security system will not reveal any information about that original plain text.

KEYWORDS: Geo-encryption, Armstrong number, GPS co-ordinates, AES

I. INTRODUCTION

There are lot of methods available to encrypt the data for security. However, these methods are location-independent. The sender cannot restrict the location of the receiver for data decryption. If the data encryption algorithm can provide such function, it is useful for increasing the security of data transmission in the future. Therefore, a Location-Dependent Data Encryption Algorithm (LDEA) is proposed. Firstly, we need an encryption algorithm and latitude and longitude of the receiver's location. The receiver can decrypt the file when the coordinates acquired by GPS devices are matched with the target coordinates. AES is one of the best encryption algorithms in terms of data safeguard and gives a high level of confidentiality as compared to DES and RSA encryption algorithm.

A GPS tracking unit is a device that uses the Global Positioning System to determine the precise location of a vehicle, person, or other asset to which it is attached and to record the position of the asset at regular intervals. The recorded location data can be stored within the tracking unit, or it may be transmitted to a central location data base, or internet-connected computer, using a cellular (GPRS), radio, or satellite modem embedded in the unit

A GPS tracking system can work in various ways. From a commercial perspective, GPS devices are generally used to record the position of vehicles as they make their journeys. Some systems will store the data within the GPS tracking system itself (known as passive tracking) and some send the information to a centralized database or system via a A GPS tracking system can work in various ways. From a commercial perspective, GPS devices are generally used to record the position of vehicles as they make their journeys. Some systems will store the data within the GPS tracking system itself (known as passive tracking) and some send the information to a centralized database or system via a modem within the GPS system unit on a regular basis (known as active tracking).

II. GPS METHOD OF OPERATION

GPS Receiver calculates its position by carefully timing the signals sent by the constellations of GPS Satellites high above the earth .Each Satellite continually transmits messages containing the time the message was sent, a precise orbit for the satellite sending the message (the ephemeris), and the general system health and rough orbits of all GPS satellites (the almanac).These signals travel at the speed of light through outer space and slightly slower through the atmosphere .the receiver uses the arrival time of each message to measure the distance to each satellite thereby establishing that the GPS receiver is approximately on the surfaces of sphere centered at each satellite . The GPS receiver also uses, when appropriate, the knowledge that the GPS receiver is on or near the surface of the sphere centred at the earth center. This information is then used to estimate the position of the GPS receiver as the intersection of sphere surfaces. The resulting co-ordinates are converted to a more convenient form for the user such as latitude and longitude, or location on a map and then displayed. It might seen that the three sphere surfaces would be enough to solve for position, since space has three dimensions. However a fourth condition is needed for two reasons. One as to do with position and the other is to correct the GPS receiver clock. It turns out that three spheres surfaces usually intersect in two points. Thus a fourth sphere surface is needed to determine which intersection is the GPS receiver position.

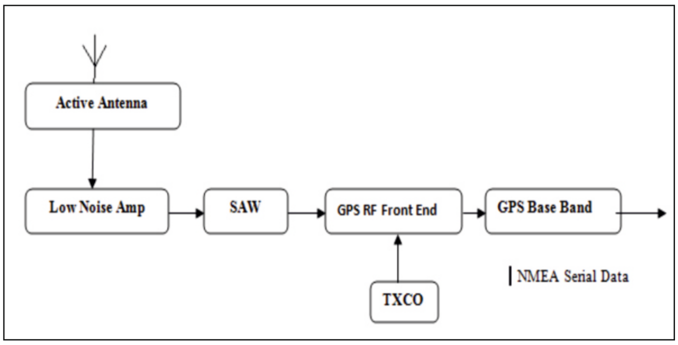

FIG 1: GPS BLOCK DIAGRAM

The GPS receiver consists of two units, first is active antenna which receives RF signals and amplifies it. The antenna is active in the sense it takes power from the module and amplifies the signal for high sensitivity. The RF signal is filtered and processed to generate NMEA format serial data output.

GPS Frame Format:
Global Positioning System Fix Data
Example:$GPGGA,170834,4124.8963,N,08151.6838,W,1,05,1.5,280.2,M,-34.0,M,,,*59

Name	Example Data	Description
Sentence Identifier	$GPGGA	Global Positioning System Fix Data
Time	170834	17:08:34 UTC
Latitude	4124.8963, N	41d 24.8963' N or 41d 24' 54" N
Longitude	08151.6838, W	81d 51.6838' W or 81d 51' 41" W
Fix Quality: - 0 = Invalid - 1 = GPS fix - 2 = DGPS fix	1	Data is from a GPS fix
Number of Satellites	05	5 Satellites are in view
Horizontal Dilution of Precision (HDOP)	1.5	Relative accuracy of horizontal position
Altitude	280.2, M	280.2 meters above mean sea level
Height of geoid above WGS84 ellipsoid	-34.0, M	-34.0 meters
Time since last DGPS update	blank	No last update
DGPS reference station id	blank	No station id
Checksum	*75	Used by program to check for transmission errors

III. ENCRYPTION METHODS
There are various encryption methods. All of them require key (below diagram). We will be using 2 keys for the encryption:
- GPS coordinates
- An Armstrong number

We will use GPS coordinates as key. We will pre-process coordinate so as to obtain stronger key. Hashing is one pre-processing method but mathematically results in weaker key. This is due to fact that hashing always return fixed length string (also contains no special characters etc.)

We will also use the Armstrong number scheme as a key to encrypt the message. An Armstrong number of three digits is an integer such that the sum of the cubes of its digits is equal to the number itself. For example, 371 is an Armstrong number since 3**3 + 7**3 + 1**3 = 371. Write a program to find all Armstrong number in the range of 0 and 999.

FLOWCHART TO GENERATE ARMSTRONG NUMBER

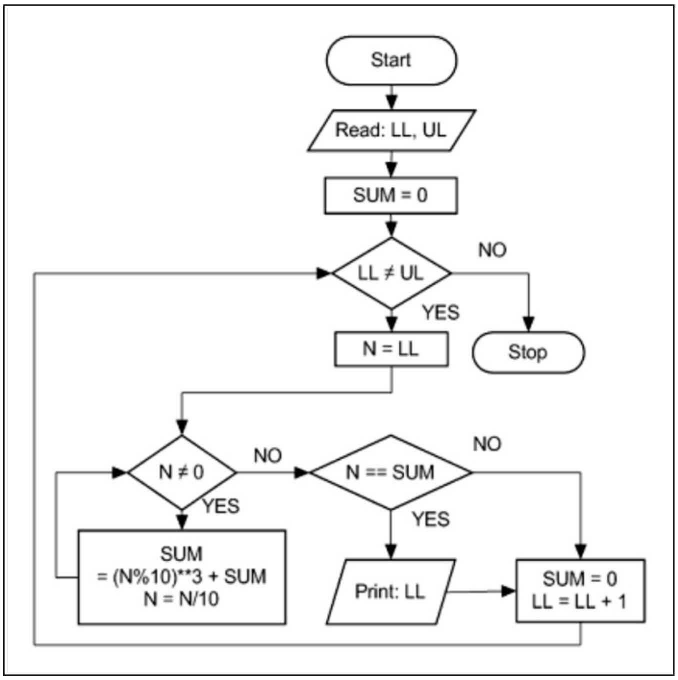

FIG 2: Armstrong Number Generation.

Working or Flow of the system:
There will be two types of users in this kind of system, one will be sender of the message and other will be the receiver of the message.

The Sender will get the GPS coordinates from receiver for its location or can decide the location coordinates where the message is supposed to be received.

Flow for sender will be as follows:
- Get target GPS coordinates manually
- Let user type the message
- Encrypt the message using step 1 as key
- Give the Armstrong Number to make the key stronger
- Let the message be transported to target location

Flow at the receiver end will be as follows:
- When message receives at target location; connect GPS module
- Get actual location from GPS; and try decryption.
- If coordinate in step 1 and 6 are same; proper encryption will occur.

IV. ALGORITHMS AND TECHNIQUES.
1. Location-Dependent Data Encryption Algorithm (LDEA)
In this algorithm the latitude/longitude coordinate is used as the key for data encryption in LDEA.

When a target coordinate is determined for data encryption, the ciphertext can only be decrypted at the expected location.

When a target coordinate is determined for data encryption, the ciphertext can only be decrypted at the expected location.

Since the GPS receiver is dependent on how many satellite signals received. It is difficult for receiver to decrypt the ciphertext at the same location exactly matched with the target coordinate. Consequently, a Toleration Distance (TD) is designed in LDEA. The sender can also determine the TD and the receiver can decrypt the ciphertext within the range of TD.

2. ADVANCED ENCRYPTION STANDARD (AES):

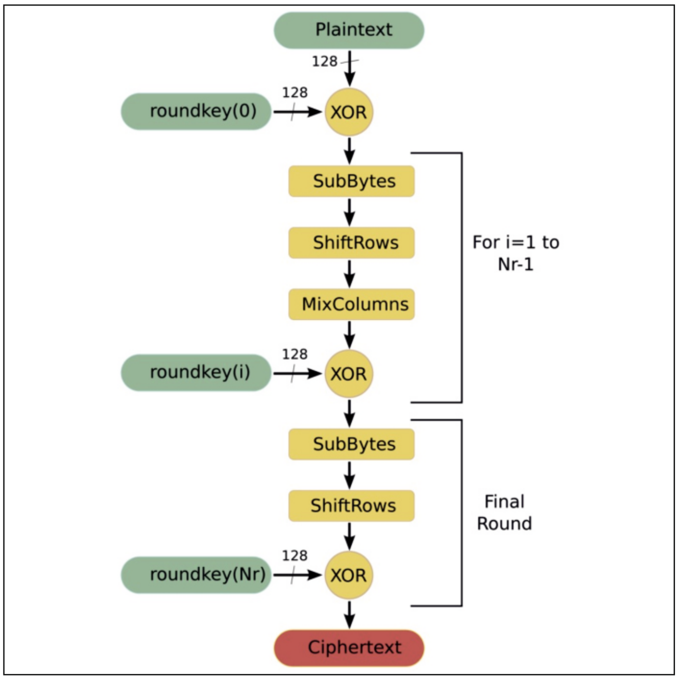

FIG 3: Working of AES algorithm.

Sub Byte Transformation SubByte operation is a nonlinear byte substitution that state bytes independently using substitution tables called the S box. The box is constructed by taking the multiplicative inverse in the Galois field (GF).

Shift Row Transformation In this step, shifting operation applies to state rows, where the first row remains as it is, second row shifted to right one time, third row shifted to the right two times and the fourth row shifted to the right three times.

Mix Column Transformation Mix column transformation carries out on the state column by column. In this operation, each byte is replaced by the value depends on all 4 bytes in the same column through the multiplication state matrix in GF.

Add Round Key Transformation The final operation in the AES round is the Add Round Key (ARK) transformation. ARK transformation is nothing but the simple bitwise XOR between state matrix and sub key.

V. FLOW GRAPHS
Sender's flow:

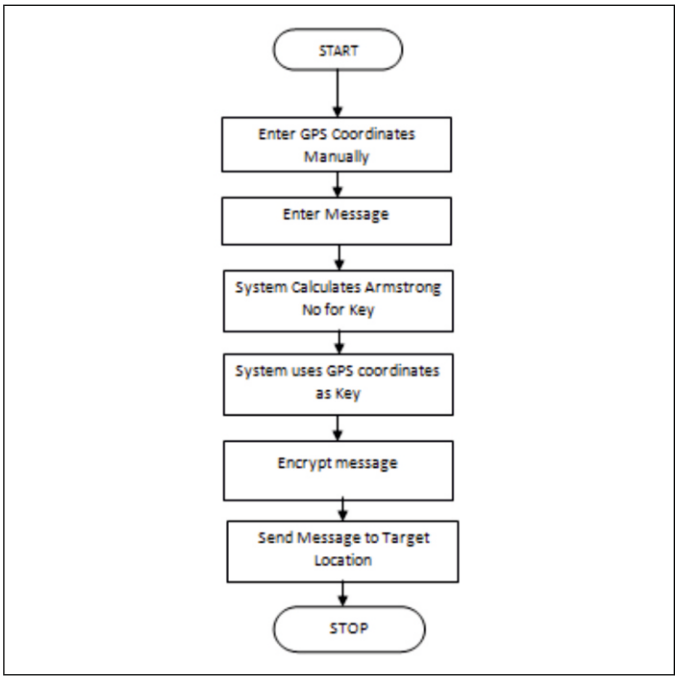

FIG 4: Sender flow

Flow for sender will be as follows:

- Get target GPS coordinates manually.
- Let user type the message.
- Encrypt the message using step 1 as key.
- Give the Armstrong Number to make the key stronger.
- Let the message be transported to target location.

Receiver's Flow:

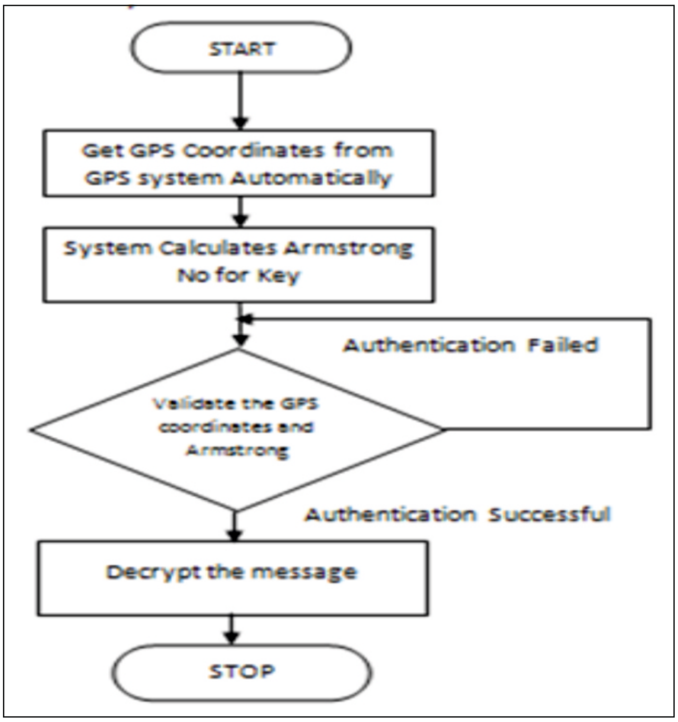

FIG 5: Receiver flow.

Flow at the receiver end is shown above in figure, FIG 5 and is explained as follows:

- When message receives at target location; connect GPS module
- Get actual location from GPS; and try decryption.
- If coordinate in step 1 and 6 are same; proper encryption will occur.

VI. METHODOLOGY

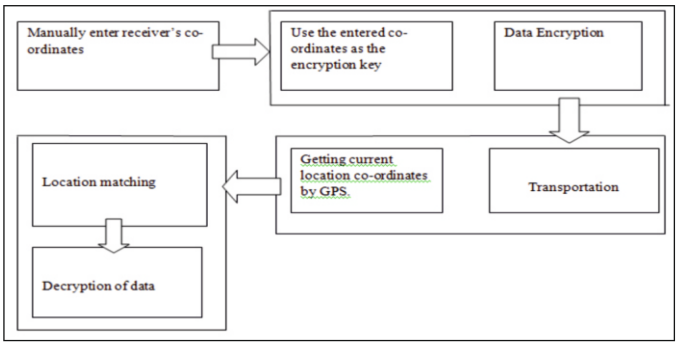

FIG 6: Methodology.

There are different cryptographic algorithms for encryption of data, but we use Advanced Encryption Standard (AES) algorithm, which will use target coordinates as key value pairs for encryption. It is used for high security and as well as for high speed. Both Hardware and software implementation are possible quite efficiently. New encryption standard is recommended by NIST (National Institute of Standards and technology) to replace DES. Encrypts data blocks of 128 bits in ten (10), twelve (12) and fourteen (14) round depending on key size as shown in Figure. It can be implemented on various platforms. It can be used in small devices. It is carefully tested for many surveillance applications.

In this module, through GPS or any other location detecting sensors coordinates of accessing devices acquired with DTD, i.e., Dynamic Tolerance Distance, which reduces the problems arises in GPS receiver in accuracy and inconsistent of data.

VII. CONCLUSION

Geo-encryption is an approach to location-based encryption that builds on established cryptographic algorithms and protocols. It allows data to be encrypted for a specific place or broad geographic area, and supports constraints in time as well as space. It can support both fixed and mobile applications, and a variety of data sharing and distribution policies. It provides full protection against location bypass. Depending on the implementation, it also can provide strong protection against location spoofing. Location's latitude/longitude co-ordinates plays vital role in the formation of encrypted data along with decryption process.

If the system software is authorized and located within a pre-defined location or area, such as for particular organization the execution of the software may achieve the location check based on proposed approach.

It provides automatic protection of sensitive files with limited delay during the initial access.

Applications:

- Military- In military this technology can be used to keep the data secured from the attackers during wars.
- Banks- This technology can also be used in banking for the purpose of money transaction.
- Individual use- It can also be used to store one's confidential data. For e.g.: for business purpose.
- Multinational Industries-In Industries important data can be secure by using this technology.
- College-In college's important data can be secure by using this technology. For e.g. Question paper.

REFERENCES

[1] D. Qiu & Sherman Lo & Per Enge & Dan Boneh, “Geoencryption Using Loran”, Proceeding of ION NTM 2007.

[2] D. Qiu, "Security Analysis of Geoencryption: A Case Study using Loran", Proceeding of ION GNSS 2007.

[3] Forouzan, "Data Communication and Networking", TMH

[4] Behrouz A. Forouzan: Cryptography and Network Security, TMH

[5] Bernard Menezes,” Network Security and Cryptography”.

[6] A.S. Tanenbaum, Computer Networks, Pearson Education.

[7] Logan Scott & Dorothy E. Denning, "Location Based Encryption & Its Role in Digital Cinema Distribution", Proceedings of ION GPS/GNSS 2003, pp 288-297.

[8] D. Denning, L. Scott, "A Location-Based Encryption Technique and Some of Its Applications", Proceedings of ION NTM 2003.

[9] Swapna B Sasi, Betsy K Abraham, JInil James, Riya Jose “Location Based Encryption using Message Authentication Code in Mobile Networks”, In IJCAT International Journal of Computing and Technology Volume 1, Issue 1, February 2014.